F: \{0,1\}^n \rightarrow \{0,1\} can be computed by a circuit of size 2. What can be computed by circuits of size Poly(n)?

AC^0: bounded depth circuits, "nots" don't count (as they can be pushed out)

Fix the depth d.

(Yet allow and/or gates with unlimited fanning)

Examples: Addition is in AC^0, multiplication isn't.

DVF: an or of many ands.

**Thm (1981, Furst, Saxe, Sipser)** the total parity is not in AC^0.

**Thm (1989, Linial-Mansour-Nisan)** if F is in AC^0, it can be approximated in l2 using low degree polynomials: For every t, there's a degree t polynomial P_s.t.

\[ \| F - P \|_2 \leq 2 \sqrt{\text{size of } F} \]

**Def** k-wise indep. dist on \{0,1\}^n is a dist. \mu all of whose k-coordinate restrictions are uniform.

Q: When do k-wise independent distributions "look random" to AC^0 circuits?

\[ \left| E_{\mu}(F) - E_{\text{uniform}}(F) \right| \leq \epsilon \forall F \in \text{AC}^0 \]

**Conjecture (Linial-Nisan 1990)** \( k = (\log(n))^{o(d)} \)

Braunman (2009): \( k = (\log(n))^{o(d)} \) is enough.

**Strategy:** "Sandwiching Polynomials":

\[ \text{Fix } F \]
$f_1, f_n$: degree $k$ polys, $f_0 \leq F \leq f_n \sum_{x \in \{0,1\}^k} |f_1(x) - f_n(x)|^2$

Claim: If $f_1, f_n$ exist, $F$ fools $\mu$. 4:49